EM radiation analysis on true random number generators: Frequency and localization retrieval method

Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer

EM radiation analysis on True Random Number Generators: Frequency and localization retrieval method

Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer
University of Lyon, Hubert Curien Laboratory, CNRS 5516, 42000, Saint-Etienne, France
pierre.bayon@univ-st-etienne.fr

***Abstract*—True random number generators (TRNGs) are significant piece of hardware security that are used to generate secret keys, initial values or random masks for counter measures against side-channel attacks. Thus the security of implementation in hardware of such block is crucial. The work presented in this paper show that it is possible to find information on a TRNG using its electromagnetic radiations. The proposed analysis is suitable to retrieve information on the localization, oscillator frequency and sampling frequency of the TRNG.**

***Index Terms*—Ring Oscillator, TRNG, EM radiation analysis, Passive attack, Near-field**

I. Introduction

Side channel attacks (SCA) are one of the major threat to hardware cryptographic systems. When an attacker is targeting a cipher to retrieve the secret key, she could perform a global attack using power analysis (PA - [1]) or electromagnetic analysis (EMA - [2]). However, these global attacks are ineffective in the presence of countermeasures that make the key not correlated with the global leakage of the chip. On the other hand, these countermeasures are not efficient if the measurement of the side channel is done locally. For example, this local measurement could be done by probing directly the chip, but this measurement is highly invasive. Using the near-field EM radiation of the chip to perform such local attack gives good results without opening the package of the device. It also permits at the same time, to build a map of the elements composing the chip ([3],[4]).

Our target in this paper will be true random number generators (TRNGs). TRNGs are essential in cryptography systems. They are used to generate random bitstream, that can be used, for instance, as confidential keys, random masks for countermeasures against SCA. Thus, the security of TRNGs is crucial.

In this paper we are proposing an attack that use the near-field EM radiation analysis of a circuit that embeds a Ring Oscillator-TRNG (RO-TRNG). The analysis is based on the study and comparison of the frequency spectrum of the EM radiations at different working conditions (e. g. power supply voltage, temperature). The results show that the proposed analysis of the device EM radiations can be used efficiently to retrieve crucial information on the TRNG. This information can be later used to help performing active attack on the TRNG such as the attack presented in [5].

The paper is organized as follows. Section II presents the test bench and the TRNG used. In section III, the proposed EM differential frequency analysis is detailed. Finally, Section IV provides experimental results demonstrating the effectiveness of the EM differential frequency analysis.

II. Case Study

A. RO-TRNG

A jittery clock generated by a RO is the most common type of source of randomness used in TRNGs. ROs are easy to implement in both ASICs and FPGAs. Figure 1 presents one of the most common TRNG principles employing several ROs. One of such TRNG was proposed in [6] and enhanced in [7]. It needs only inverters (for implementing ROs), flip-flops (as samplers) and a large XOR gate (entropy collector). In [6], authors proposed a mathematical model of the TRNG that guarantees enough entropy in the output bit and thus the robustness and security. This kind of generator is widely use in industrial application.

The generator has several parameters that can be tuned: number of inverters composing ROs, number of ROs and the sampling frequency. Modifying these parameters, the designer can change the statistical properties of the random bitstream produced by the TRNG. For example, according to [7], for a sampling frequency of 100 MHz, the generator composed of 25 ROs, each using 3 inverters, generates the bitstream passing common statistical tests even without post-processing.

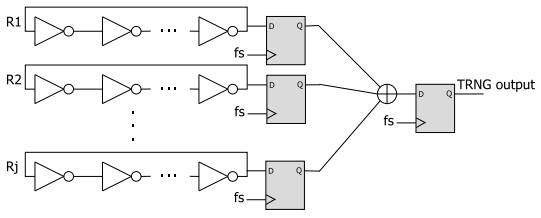

Fig. 1. RO-TRNG.

B. Test Bench

The EM radiation of the device is evaluated using a near-field ($\sim\leq$ 23mm) EM analysis test bench from Fig. 2. The most important part of the test bench is the acquisition chain.

It determines the signal to noise ratio and precision of the measurement. It is composed of:

- A Rhode and Schwarz magnetic probe with the frequency range from 100 kHz to 3 GHz and the spatial resolution of approx. 500 μm.
- A Miteq low-noise amplifier with the frequency range from 100 MHz to 2 GHz.
- A Lecroy oscilloscope with the frequency range up to 3.5 GHz.

The device under test (the board) is fixed on a XYZ table with repeatability of movement of 1 μm. The test bench, including acquisition chain, XYZ table, FPGA configuration and power supply variations, is controlled by a PC. Note that, compared to typical EM compatibility analysis, we did not need to use a faraday cage to protect the measurement chain from EM interference.

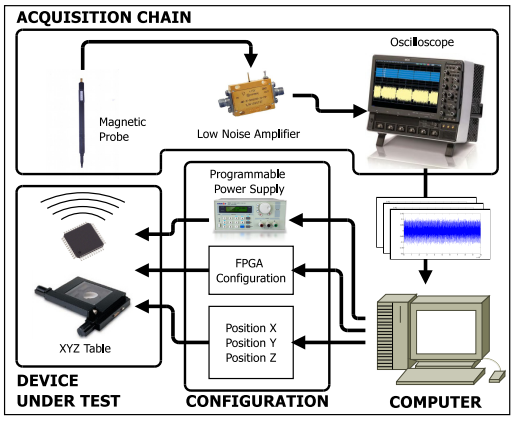

Fig. 2. EM analysis test bench

III. EM Analysis Applied to a RO-TRNG

A. Frequency Analysis

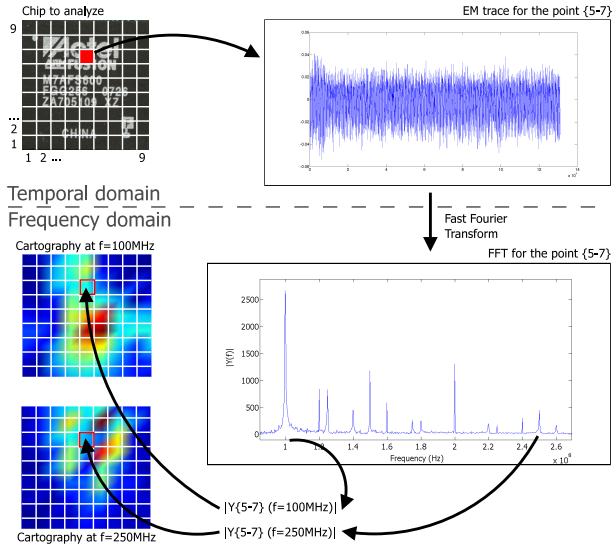

Fig. 3. EM cartography using frequency analysis

The goal of the passive attack is to retrieve as much information as possible on the cryptographic system and namely on the TRNG. When using RO-TRNG, we suppose that the attacker will tend to determine the working frequencies of the ROs, their locations on the chip, and if possible, the sampling frequency of the flip-flops. To extract such an information from the EM radiations, we have used a so-called EM cartography method presented in Fig. 3. In this method, the EM radiations of the device are analyzed point by point using a frequency analysis [3]. The aim of the EM cartography is to obtain an EM map of the device at certain frequency (e. g. see two maps on the left side of Fig. 3, one obtained at 100 MHz and the second one at 250 MHz). For each point (i, j), an electromagnetic trace is acquired and the power spectral density (PSD) of this trace denoted $|Y\{i,j\}(f)|$ is computed using Fast Fourier Transform (FFT). Figure 4 presents a typical PSD of the EM radiation of a cryptographic circuit including a RO-TRNG embedded in an FPGA. Notice that it is not possible to directly guess the ROs working frequencies. Indeed, the RO-TRNG represents a small part of the cryptographic system and its contribution to the EM radiation is insignificant compared to the contribution of large synchronous blocks such as cipher. As a consequence, the attacker will need to discern the frequency contributions of the ROs from those of the other modules in the PSD.

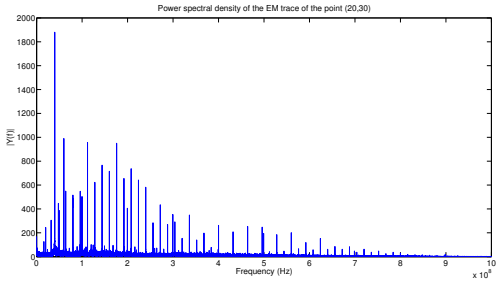

Fig. 4. Typical Power spectral density of the EM traces at a random location in the EM device map

B. Differential Frequency Analysis

It is commonly known that the RO frequency depends dynamically on the power supply voltage and temperature. In synchronous systems clocked by an external quartz oscillator (most of today's systems), the frequency of RO is more sensitive to environmental variations than that of the system clock. This RO characteristic can be used to discern ROs frequency contributions in the PSD by performing a differential frequency analysis. This analysis consists in performing two successive EM frequency analyses for two distinct working conditions {Cond #1, Cond #2} (e. i. two distinct power supply voltages or two distinct temperatures). A differential EM radiation PSD is computed by subtracting the two PSD at Cond #1 and Cond #2. This differential PSD is expected to contain two symmetrical spectral contributions with large frequency shifting, which highlights the presence of condition-sensitive block such as RO in the targeted chip. Final EM

device maps at Cond #1 and Cond #2 permit to detect the presence of ROs and determine its location and frequency.

C. Experiments

We realized three experiments:

- The first two experiments should show that the proposed method is suitable to detect a RO-TRNG, while an AES (using a 20MHz clock) is running in the same device (one RO-TRNG in the upper left corner in Experiment #1 and one in the lower right corner in Experiment #2, as shown in Fig. 5).
- The third experiment aim at proving that it is possible to find the sampling frequency of the RO-TRNG. It consists of using design of experiment#2 and doing measurement for two different sampling frequencies.

We have implemented the two designs in the Microsemi Fusion AFS600 FPGA device. The TRNG was built using 50 ROs, each composed of 3 inverters. For the first two experiments the sampling frequency was 6.9 MHz. For the third one we used two sampling frequencies: 6.9 MHz and 8.9 MHz. We recall that the EM analysis is not invasive and so the FPGA package could remain intact.

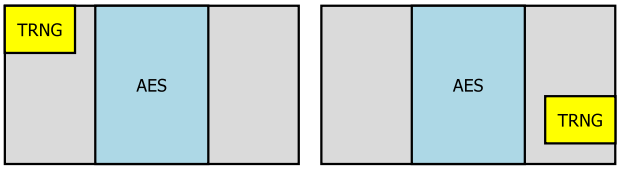

Fig. 5. From left to right floorplan of: Experiment #1and Experiment #2

We decided to perform the EM cartography of the whole FPGA package (1.7 cm x 1.7 cm). In order to get a sufficient resolution and to have a reasonable amount of points, we have chosen a resolution of 90x90 points ($\sim$ 200 μm resolution). For each point of the EM device map, 10 traces of 200 000 points (with a sampling rate of 20 Gsa/s) were acquired and then averaged. In order to simplify the analysis (obtention of the RO's frequency range), the points were gathered in 9 larger "areas" (30x30), for which the PSDs are averaged. Note that for localizing ROs, the map resolution remains unchanged.

As stated previously, in the differential frequency analysis, the attacker needs to obtain two EM device maps at different voltage or temperature conditions. It is important to note that the working conditions (voltage or temperature) must remain sufficiently stable during the construction of each of two EM device maps. We decided to modify the power supply voltage of the device because it was more accurate than varying temperature. The EM device maps are performed at 1.5 V and 1.7 V for the Experiment #1 and #2.

IV. Experimental Results

A. Results of Experiment #1 and #2: RO frequency and localization retrieval

The PSDs of the first two experiments are depicted in Fig. 6 and Fig. 7. We recall that the aim of the first two experiments was to show that it is possible to find the position and frequencies of the ROs composing a RO-TRNG while an AES is running in the same device. In section III.B we expected that only the frequencies corresponding to the ROs would clearly appear in the differential PSDs. As it can be seen in Fig. 6 and Fig. 7, other frequencies are not completely suppressed by the differential frequency analysis. This is mainly due to the fact that, for a given system frequency, the amplitude of this frequency in the PSD varies slightly from one measurement to another. Nevertheless, this effect remains negligible and the proposed method remains very useful for locating frequencies of interest in the PSDs.

In Fig. 6 and Fig. 7, the positive part of the differential PSDs corresponds to the EM device map at 1.5 V and the negative part to the EM device map at 1.7 V.

For Experiment #1 (see Fig. 6):

- For 1.5 V, ROs frequencies range from 331 to 354 MHz.
- For 1.7 V, ROs frequencies range from 376 to 399 MHz.

From Fig. 6, we can expect that the RO-TRNG radiation will be visible in the upper left corner of the DIE only for the couple of conditions (1.5 V and f = [331 MHz - 354 MHz]) and (1.7 V and f = [376 MHz-399 MHz]).

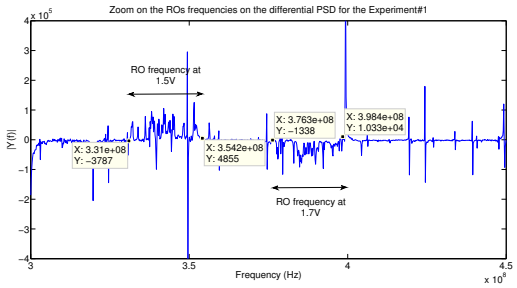

Fig. 6. Differential PSD of the Experiment #1 at the center of the chip

For Experiment #2 (see Fig. 7):

- For 1.5 V, ROs frequencies range from 327 to 347 MHz.
- For 1.7 V, ROs frequencies range from 374 to 394 MHz.

From Fig. 7, we can expect that the RO-TRNG radiation will be visible in the bottom right corner of the DIE only for the couple of conditions (1.5 V and f = [327 MHz - 347 MHz]) and (1.7 V and f = [374 MHz-394 MHz]).

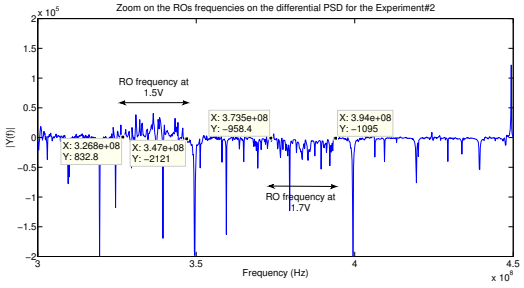

Fig. 7. Differential PSD of the Experiment #2 at the center of the chip

Figure 8 and Fig. 9 show EM device maps of Experiment #1 and #2 for the two power supply voltage conditions (1.5 V

and 1.7 V). The white dotted rectangle represents the FPGA's DIE and the solid rectangle represents the location of the ROs. These EM device maps are plotted for the frequencies ranges obtained by the differential frequency analysis. We can conclude that we are able to locate the RO-TRNG on the chip by finding the RO's working frequencies. Plus we can note that the activity of the AES block inside the FPGA has no influence on the result of the EM differential frequency analysis.

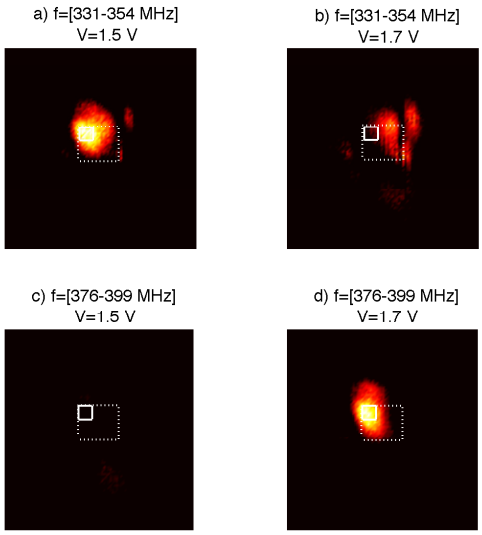

Fig. 8. EM device maps for the Experiment #1

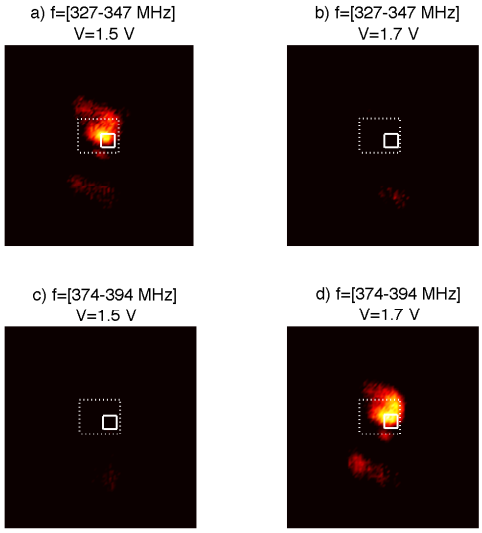

Fig. 9. EM device maps for the Experiment #2

B. Results of Experiment #3: Sampling frequency retrieval

The aim of this experiment is to retrieve the sampling frequency of the RO-TRNG. The figure Fig. 10 depicts the differential PSD for the whole circuit (all the PSDs were averaged) between a measurement for a sampling frequency of 8.9 MHz (positive part of Fig. 10) and a measurement at 6.9 MHz (negative part). It is then easy to find out the sampling frequency of the RO-TRNG, in fact the attacker just has to find frequency peaks that will be repeated, with the same spacing, all over the PSD trace. Thus, the sampling frequency will be this spacing.

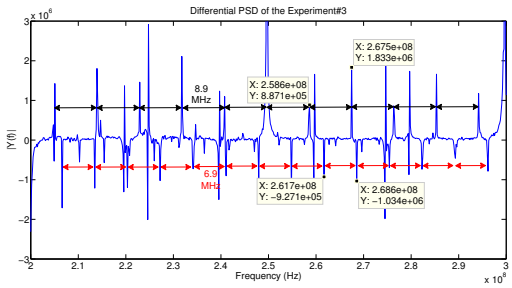

Fig. 10. Differential PSD of the Experiment #3 for the whole circuit

V. Conclusion

Using our EM differential analysis of the frequency we were able to find the localization of a RO-TRNG in an FPGA package while running a complete crypto-system in it. The proposed analysis is also suitable to determine the RO frequency and the sampling frequency of the TRNG, that could be helpful to tune an active attack later on. As proposed in the paper, our analysis requires a small modification of the power line of the board, since we need to modify the voltage of the FPGA core, but this analysis could be completely non invasive if the attacker, for instance, has the possibility to precisely heat up the device and maintaining the temperature during the whole acquisition.

References

[1] P. C. Kocher, J. Jaffe, and B. Jun, Differential Power Analysis", Advances in Cryptology - CRYPTO 99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings, ser. Lecture Notes in Computer Science, vol. 1666. Springer, 1999, pp. 388397.

[2] K. Gandolfi, C. Mourtel, and F. Olivier, Electromagnetic Analysis: Concrete Results, in Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings, ser. Lecture Notes in Computer Science, C . K. Koc, D. Naccache, and C. Paar, Eds., vol. 2162. Springer, May 2001, pp. 251261.

[3] L. Sauvage, S. Guilley and Y. Mathieu, "Electromagnetic Radiations of FPGAs: High Spatial Resolution Cartography and Attack on a Cryptographic Module", ACM Transactions on Reconfigurable Technology and Systems, 2009, Vol. 2, No. 1, Article 4.

[4] D. Réal, F. Valette, and M. Drissi, Enhancing correlation electromagnetic attack using planar near-field cartography", in Design, Automation and Test in Europe, DATE 2009, Nice, France, April 20-24, 2009. IEEE, 2009, pp. 628633.

[5] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson and P. Maurine "Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator", Constructive Side-Channel Analysis and Secure Design (COSADE2012), 2012, pp. 151-166.

[6] B. Sunar, W.J. Martin and D.R. Stinson, "A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks", IEEE Transactions On Computers, 2007, vol. 56, no. 1, pp. 109-119.

[7] K. Wold and C. H. Tan, "Analysis and Enhancement of Random Number Generator in FPGA based on Oscillator Rings", International Conference on Reconfigurable Computing and FPGAs (ReConFig'08), 2008, pp. 385-390.